REMARKS

I. Status of Claims

Claims 1-5 and 8-11 have been amended.

Claims 1-12 are thus pending in the application.

In the Office Action, claims 2 and 3 were objected because of informalities.

Claims 1-5 and 7-10 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Applicant's admitted prior art (AAPA) in view of 3rd Generation Partnership Project, "Document 2: KASUMI Specification" Release 4, 2001-08-28 (DKS) and further in view of U.S. Patent No. 6,324,288 to Hoffman.

Claims 6, 11 and 12 were also rejected under 35 U.S.C. § 103(a) as being unpatentable over AAPA in further view of DKS, Hoffman and U.S. Patent No. 4,304,961 to Campbell, Jr.

II. Claim Objections

The Examiner objected to claims 2 and 3 because of informalities.

With respect to claim 2, the Examiner asserted that the claim recites "**second** encryption codes comprises at least one of $KO_{1,1}$, $KO_{1,2}$, $KO_{1,3}$, $KI_{1,1}$, $KI_{1,2}$ and $KI_{1,3}$." Applicant respectfully submits that claim 2 has been amended to recite "**first** encryption codes comprises at least one of $KO_{1,1}$, $KO_{1,2}$, $KO_{1,3}$, $KI_{1,1}$, $KI_{1,2}$ and $KI_{1,3}$."

With respect to claim 3, the Examiner asserted that the claim recites "the first predetermined encryption codes comprises at least one of $KO_{2,1}$, $KO_{2,2}$, $KO_{2,3}$, $KI_{2,1}$, $KI_{2,2}$ and $KI_{2,3}$." Applicant respectfully submits that claim 3 has been amended to recite "the predetermined **second** encryption codes comprises at least one of $KO_{2,1}$, $KO_{2,2}$, $KO_{2,3}$, $KI_{2,1}$, $KI_{2,2}$ and $KI_{2,3}$.

III. Rejections under 35 U.S.C. § 103(a)

a. The Examiner rejected claims 1-5 and 7-10 under 35 U.S.C. § 103(a) as being unpatentable over Applicant's admitted prior art (AAPA) in view DKS and further in view of Hoffman.

With respect to independent claim 1, the combination of AAPA, DKS and Hoffman, taken singly or in combination, does not disclose or teach a method for "performing a second-round of encryption by encrypting the received first operated ciphertext bit steam and the second operated ciphertext outputting the third and fourth ciphertext bit streams after receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream comprising the predetermined time delay and generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit steam and the second operated ciphertext bit stream with predetermined second encryption codes," as recited in amended claim 1.

AAPA discloses an example of FOi units, where FOi denotes an ith FO unit. However, the FO2 unit 220 does not encrypt a received first operated ciphertext bit stream. FL1 unit (110) in Figure 1 of AAPA outputs a first 32-bit ciphertext (L_{01}). **FO1 unit 210 encrypts the first 32 bit ciphertext (L_{01})** and outputs a second ciphertext (L_{02}). An exclusive-OR operation is performed on the second ciphertext (L_{02}) and a 32-bit signal R_0 to provide a 64 bit ciphertext. The 64-bit ciphertext is received and encrypted in FO2 unit 220 using encryption keys KO_2 and KI_2. *See* page 2, lines 4-18 of the specification. The Examiner alleged that Figure 2B teaches the implementation of FO2 unit 220. However, Figure 2B receives **a 32-bit signal** and FO2 unit 220 receives **a 64-bit ciphertext.**

The Examiner acknowledges that in Figure 2B, $L_{0'}$ reads on a first operated ciphertext bit stream and $R_{0'}$ reads on a second operated ciphertext bit stream. The Examiner also acknowledges that the output of the first round of encrypting (Figure 1, 220) combined with R_0 by performing an exclusive-OR operation causes a time delay.

AAPA discloses in Figure 2B a **16-bit signal $L_{0'}$** and another **16-bit signal $R_{0'}$** (not first and second ciphertext bit streams as indicated by the Examiner). *See* page 3, lines 25-27 and page 2, lines 24 (referencing L_0 and R_0 as two 16-bit signals generated by dividing a 32-bit input signal). Moreover, the exclusive-OR performed in Figure 1 on R_0 and L_{02} does not cause a time delay. The exclusive-OR operation is a logic operation on two operands that result in a logical value and not a time delay.

AAPA further discloses a first operated ciphertext bit stream ($R_{3'}$), generated by an exclusive-OR operation performed on signal $L_{2'}$ and a 16-bit sub-encryption key $KO_{1,3}$, and a second operated ciphertext bit stream ($L_{3'}$), generated by an exclusive-OR operation performed on signal $L_{1D'}$ from $F1_{1',1'}$ subcipher and delayed signal $R_{1D'}$. The first and second operated ciphertext bit streams of Figure 2B are encrypted with first encryption codes and not second encryption codes (first encryption codes $KO_{1,1}$, $KO_{1,2}$, $KO_{1,3}$, $KI_{1,1}$, $KI_{1,2}$ and $KI_{1,3}$ are only used in Figure 2B). Accordingly, there is nothing in AAPA that discloses or teaches performing a second-round of encryption by encrypting the received first operated ciphertext bit steam and the second operated ciphertext bit stream comprising the predetermined time delay **with predetermined second encryption codes an odd number of times**.

AAPA also discloses in Figure 2B a third operated ciphertext bit stream $R_{4'}$ and a fourth operated ciphertext bit stream $L_{4'}$. However, there is nothing in Figure 2B of AAPA that discloses or teaches concurrently outputting the third and fourth ciphertext bit streams of length n **after encrypting the first operated ciphertext bit stream again with the predetermined second encryption codes**. The first operated ciphertext bit stream $R_{3'}$ in Figure 2B is not encrypted again. Moreover, the first operated ciphertext bit stream $R_{3'}$ in

Figure 2B is not encrypted with second encryption codes. First encryption codes $KO_{1,1}$, $KO_{1,2}$, $KO_{1,3}$, $KI_{1,1}$, $KI_{1,2}$ and $KI_{1,3}$ are only used in Figure 2B.

The Examiner acknowledged that AAPA fails to explicitly disclose performing encryption of first and second ciphertext bit streams at the same time; and utilizing predetermined second encryption codes. To cure the deficiencies of AAPA (namely, Figures 2A and 2B), the Examiner relied on DKS for illustrating that using second set of predetermined encryption codes for a second round of encryption is standard in a Kasumi encryption algorithm, by referencing page 12, second 4.3 and page 10, section 2.3, line 10.

DKS discloses subkeys KL_i, KO_i, and KI_i that are used in an ith round of a KASUMI algorithm. Even if, assuming *arguendo*, the subkeys of DKS are combined with AAPA (namely, Figures 2A and 2B), the encryption keys would be inoperable within the FO1 unit. Figures 2A and 2B comprise the FO1 unit with first encryption codes. However, if Figures 2A and 2B each represented FO2 unit 220, second encryption codes KL_2, KO_2 and KI_2 are then used. However, FO2 unit 220 can not be used in Figures 2A and 2B because FO2 unit 220 receives a 64-bit signal that was generated from an exclusive-OR function on a 32-bit signal R_0 and a 32-bit ciphertext L_{02} (which is a second ciphertext) and encrypts the 32-bit ciphertext L_{02}. The FO1 units of Figures 2A and 2B receives a 32-bit signal. Also, the FO2 unit 220 does not encrypt a received first operated ciphertext bit stream and a second operated ciphertext bit stream comprising a predetermined time delay. Moreover, the FO2 unit 220 does not encrypt an odd number of times.

To further cure the deficiencies of AAPA, the Examiner relied on Hoffman for disclosing a method of performing encryption of first and second ciphertext bit streams at the same time.

Applicant respectfully submits that the recitations of the claim 1 does not recite performing encryption of first and second ciphertext bit streams at the same time. The claim recites "generating a first operated ciphertext bit stream . . . at the same time of performing encryption of the second ciphertext bit stream." Accordingly, the use of the Hoffman reference is moot, since Hoffman does not supply any of the other above-noted deficiencies.

In view of the above arguments, the combination of AAPA, DKS and Hoffman, taken singly or in combination, does not disclose or teach claim 1. Therefore the rejection of claim 1 should be withdrawn. The rejection of claim 8, which recites "a second ciphering unit for receiving the first operated ciphertext bit stream and the second operated ciphertext bit stream comprising the predetermined time delay, generating third and fourth ciphertext bit streams of length n by encrypting the first operated ciphertext bit stream and the second operated ciphertext bit stream with at least one of predetermined second encryption codes $KO_{2,1}$, $KO_{2,2}$, $KO_{2,3}$, $KI_{2,1}$, $KI_{2,2}$, and $KI_{2,3}$ an odd number of times, and concurrently outputting the third and fourth ciphertext bit streams after encrypting the first operated ciphertext bit stream again with the predetermined second encryption codes," should be withdrawn for at least the same reasons given for independent claim 1. Moreover, claims 2-5, 7, 9, 11 and 12, which incorporate the limitations of base claims 1 and 8, should also be withdrawn at least based on the above arguments for claim 1. Likewise, Campbell, Jr. does not supply at least the above-noted deficiencies of AAPA, DKS, and Hoffman.

b. The Examiner rejected claims 6, 11 and 12 under 35 U.S.C. § 103(a) as being unpatentable over AAPA and further in view of DKS, Hoffman and Campbell, Jr.

With respect to claim 6, the Examiner acknowledged that neither AAPA and DKS nor Hoffman explicitly disclose the outputs from the first and second sub-encryptions are stored and simultaneously retrieved according to an external clock signal. To cure the deficiencies of AAPA, DKS and Hoffman, the Examiner relied on Campbell, Jr. as disclosing **the outputs** are stored and simultaneously retrieved according to an external clock (by referencing Figure 1A, reference numeral 18, 20 and 22; Figure 2; column 5, lines 66-68 and column 6, lines 1-7 and 11-16).

Campbell, Jr. discloses a device for generating an authenticator code by encrypting contents of a plain text message in accordance with a unique user supplied authenticator key variable. Campbell, Jr. also discloses a T1 memory (20), loaded with a 16-bit authenticator key variable contained in a K memory (48), that serves as an address input to T2 memory (24), and a T3 memory (18) in which data read out of the T3 memory (18) is combined with six low order bits from a shift register in an exclusive OR gate (26) used to replace previous six low order bit positions of a shift register (14) from a control sequencer (22). The control sequencer 22 controls a read cycle initiated at each memory (see col. 5, line 55 – col. 6, line 34). There is nothing in Campbell, Jr. that discloses an encryption method in which **each of the encryptions includes first and second sub-encryptions**. Moreover, there is nothing in Campbell Jr. that discloses that the authenticator key variable provided in T1 memory (20) comprises **first and second sub-encryptions**.

In view of the above arguments, the combination of AAPA, DKS, Hoffman and Campbell, Jr. does not disclose or teach the claimed elements of claim 6. Therefore, the rejection of claim 6, which incorporates the limitations of base claim 1, should be withdrawn for at least the same reasons give above with regard to claim 1.

CONCLUSION

Applicant submits that the above amendments and arguments are fully responsive to the Office Action dated June 26, 2007 and respectfully requests the asserted grounds of rejections be withdrawn based on such arguments.

In view of the above, it is believed that the above-identified application is in condition for allowance, and notice to that effect is respectfully requested. Should the Examiner have any questions, the Examiner is encouraged to contact the undersigned at the telephone number indicated below.

Respectfully submitted,

Demetra Smith-Stewart

Demetra Smith-Stewart
Attorney of Record
Reg. No. 47,354

Roylance, Abrams, Berdo & Goodman, L.L.P.
1300 19th Street, N.W., Suite 600
Washington, D.C. 20036-2680
(202) 659-9076

Dated: September 25, 2007